THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL. XIX. MARCH, 1912. NO. 3.

ON THE SUM OF THE NUMBERS WHICH BELONG TO A FIXED EXPONENT AS REGARDS A GIVEN MODULUS.

By G. A. MILLER, University of Illinois.

§ 1. INTRODUCTION.

In article 81 of Gauss's *Disquisitiones Arithmeticae*, 1801, it is proved that the sum of the incongruent primitive roots of a prime number p is $\equiv 0 \pmod{p}$ whenever $p-1$ is divisible by the square of a prime; when $p-1$ is not divisible by the square of a prime, this sum is $\equiv 1$ or $\equiv -1$ according as $p-1$ is the product of an even or of an odd number of distinct primes. As this theorem can be so readily verified it is within easy reach of those whose mathematical attainments are very meagre. We proceed to illustrate it by using successively for p the numbers 13, 11, and 31.

The four primitive roots of 13 are 2, 6, 7, 11. Their sum is $26 \equiv 0 \pmod{13}$ and 12 is divisible by 2^2. The four primitive roots of 11 are 2, 6, 7, 8. Their sum is $23 \equiv 1 \pmod{11}$ and 10 is the product of two distinct primes. The eight primitive roots of 31 are 3, 11, 12, 13, 17, 21, 22, 24. Their sum is $123 \equiv -1 \pmod{31}$ and 30 is the product of an odd number of distinct primes.

The given theorem, due to Gauss, has been proved in various ways and was extendod by Arndt in 1846.* In Bachmann's *Niedere Zohlentheorie*, 1902, page 333, we find the following much more general theorem: The sum of the incongruent numbers which belong, with respect to mod p^α or mod $2p^\alpha$ (p being any odd prime), to any exponent which is divisible by the square of a prime is always $\equiv 0$; when this exponent is not divisible by the square of a prime, the given sum is $\equiv 1$ or $\equiv -1$ according as the exponent is the product of an even or of an odd number of distinct primes.

As It is so very easy to verify that this general theorem is not universally true it is singular that it should have appeared in such an excellent work, even if it is corrected in the Zusatze at the end of the volume. For instance, if we let $p \equiv 3$ and $\alpha \equiv 3$, it is evident that 10 and 19 are the two incongruent numbers which belong to exponent 3. Their sum is $29 \equiv 2 \pmod{27}$

Journal für die riene und Angewandte Mathematik, Vol, 31.

instead of being $\equiv -1$ in accord with the general theorem. On the other hand, the six incongruent numbers which belong to exponent 9 (mod 27) are as follows: 4, 7, 13, 16, 22, 25. Their sum is $87 \equiv 6$ instead of being $\equiv 0$ in accord with this theorem.

In the present paper we aim to give a few new theorems relating to the sum of the numbers which belong to a given exponent, to give a simple proof of the generalization of Gauss's theorem due to Arndt, and also to exhibit clearly some relations between number theory and group theory which are connected with particular developments. Various points of contact between these two theories have been noted before, but their common ground doubtless offers still much to be investigated. It may be remembered that Poincaré called particular attention to the fact that the borderlands between various mathematical fields give the greatest promise for important advances.*

§ 2. Theorems Relating to a General Modulus.

It is well known that the $\phi(m)$ positive integers which do not exceed the positive integer m and are prime to it constitute an abelian group G with respect to multiplication (mod m).† These $\phi(m)$ numbers are said to constitute a reduced system of residues (mod m), and it is evident that 1 and $m-1$ belong to exponents 1 and 2 respectively. Little is known as regards the exponents of the other numbers except that each of the exponents is a divisor of $\phi(m)$.

Since $m-1 \equiv -1$ (mod m) corresponds to an operator of order 2 in G, and the products of all the operators of G by any one of them give each of these operators once and only once, it results that we obtain a reduced system of residues (mod m) by multiplying each number of such system by -1. In particular, the sum of all the numbers of any reduced system of residues (mod m) is $\equiv 0$, since this sum is not altered when we change its sign. If we multiply an operator whose order is divisible by 4 by any operator of order 2 which is commutative with it the order of this product is the same as the order of the given operator. Hence it results directly that *the sum of all the numbers of any reduced system of residues (mod m), which belong to any exponent which is divisible by 4 must always be $\equiv 0$ (mod m).*

To illustrate this theorem we may consider the reduced system of residues mod 20. The eight numbers of this reduced system are evidently as follows:

$$1, 3, 7, 9, 11, 13, 17, 19.$$

The four numbers which belong to exponent 4 are 3, 7, 13, 17. Their sum is clearly $\equiv 0$ (mod 20). It may be observed that the sum of the three

*Poincaré, *Bulletin des Sciences Mathématiques*, Vol. 43 (1908), p. 179.
†Cf. *Annals of Mathematics*, Vol. 2 (1901), p. 72.

numbers 9, 11, 19 which belong to exponent 2 is $\equiv -1 \pmod{20}$. This is a special case of the theorem: *The sum of all the incongruent numbers which belong to exponent 2 with respect to any modulus is* $\equiv -1$. This theorem follows directly from the facts that the order of the product of any two operators of order 2 in G is of order 2 and that -1 corresponds to one of these operators of order 2, since it results from these facts that a change of the signs of all the numbers, except -1, which correspond to operators of order 2 in G, does not affect this totality (mod m).

For the same reason it results that the sum of all the numbers, in any reduced system of residues, which belong to an odd exponent or to twice this exponent is always $\equiv 0$. In fact, if we multiply by -1 all those numbers which belong to any odd exponent or to twice this exponent (mod m) we obtain all those which belong to these exponents. From the theorems stated above, it follows directly that all the sum of all the incongruent numbers which belong to exponent δ mod 2^α is $\equiv 0$ or $\equiv -1$ according as $\delta > 2$ or $= 2$. This follows directly from the fact that $\phi(2^\alpha)$ is $2^{\alpha-1}$, and hence all the exponents to which odd numbers belong (mod 2^α) are powers of 2.

§ 3. Theorems Relating to a Prime Modulus.

We shall first consider the case when $p-1$, p being the prime modulus, is not divisible by the square of a prime number. Hence we have

$$p-1=p_1 p_2 \ldots p_\lambda ,$$

where $p_1, p_2 \ldots p_\lambda$ are distinct prime numbers. Since the sum of the distinct roots of the congruence

$$x^{p_\alpha} \equiv 1 \pmod{p} \qquad \alpha = 1, 2, \ldots \lambda$$

is zero, and unity is one of these roots, it results that the sum of the numbers of the series

$$1, 2, \ldots p-1$$

which belong to exponent p_α is $\equiv -1 \pmod{p}$.

To obtain the sum of those numbers which belong to exponent $p_\alpha p_\beta$ ($\alpha, \beta = 1, 2, \ldots$ or λ and $\alpha \neq \beta$), we observe that the sum of the roots of the congruence

$$x^{p_\alpha p_\beta} \equiv 1 \pmod{p}$$

is zero and that the sum of these roots which belong either to exponent p_α or to exponent p_β is -1. Hence the sum of the roots which belong to exponent $p_\alpha p_\beta$ is 1. These illustrations suffice to suggest the theorem that the sum of the numbers of the set 1, 2, . . . $p-1$ which belong to an exponent which is the product of an even number of distinct primes is $\equiv 1 \pmod p$, while the sum of these numbers is $\equiv -1 \pmod p$ when the exponent is the product of an odd number of distinct prime factors. We proceed to prove, by complete induction, that this theorem is universally true.

Suppose that this theorem is true for r distinct prime factors p_1, p_2, . . . p_r $(r<\lambda)$, and consider the congruence

$$x^{p_1 p_2 \cdots p_{r+1}} \equiv 1 \pmod p.$$

The sums of the roots which belong to a prime exponent and to an exponent which is the product of two, three . . . up to r distinct primes, are, by hypothesis, as follows:

$$-(r+1) + \frac{(r+1)\,r}{2} - \frac{(r+1)r\,(r-1)}{3!} + \cdots + (-1)^{r+1}(r+1).$$

This formula results directly from the fact that a cyclic group has one and only one subgroup whose order is an arbitrary divisor of the order of the group and that the $p_1 p_2 \cdots p_{r+1}$ roots of the congruence

$$p^{p_1 p_2 \cdots p_{r+1}} \equiv 1 \pmod p$$

form a cyclic group (mod p), when they are combined by multiplication.

The terms of the given formula are evidently all the terms, except the first and the last, of the expansion

$$(1-1)^{r+1}.$$

Since the root unity furnishes the first term of this expansion and since the sum of all the roots of the congruence under consideration is $\equiv 0 \pmod p$, it results that the sum of all those roots which belong to exponent $p_1 p_2 \cdots p_{r+1}$ is congruent to the last term of this expansion. That is, this sum is $\equiv 1 \pmod p$ when $r+1$ is even, while it is $\equiv -1 \pmod p$ when $r+1$ is odd. As the given theorem is true when $r=1$ or 2 it must therefore be universally true.

Suppose now that $p-1$ is divisible by p_α^β, p_α being a prime number and $\beta>1$. There will then be one and only one subgroup of order p_α^β in G and the numbers which correspond to the operators of this subgroup are the roots of the congruence

$$x^{p_a^\beta} \equiv 1 \pmod{p}.$$

Since the sums of these roots which satisfy each of the congruences

$$x^{p_a} \equiv 1 \pmod{p}, \quad x^{p_a^2} \equiv 1 \pmod{p}$$

are zero it results directly that the sum of those roots which belong to exponent p_a^2 is zero. If $\beta > 2$, it may be proved in a similar that the sum of those roots which belong to exponent p_a^3 is zero, etc. That is, *the sum of those numbers of the series 1, 2 . . . p—1 which belong to an exponent which is a power, greater than the first, of any prime is* $\equiv 0 \pmod{p}$.

If $p-1$ is divisible by $p_a^\beta q$, q being a prime number, and $\beta > 1$, the sum of those roots of the congruence

$$x^{p_a^\beta q} \equiv 1 \pmod{p},$$

which belong to exponent $p_a^2 q$ is $\equiv 0 \pmod{p}$, since the sum of those whose exponents divide $p_a q$ is $\equiv 0 \pmod{p}$. From this it results directly that the sum of those roots which belong to exponent $p^\delta q$, $\delta \leqq \beta$, is also $\equiv 0 \pmod{p}$, as may be seen by assigning to δ successively the values 3, 4 . . . β. Hence it results from the theorem proved above, by complete induction, that if $p-1$ is divisible by $p_a^\beta q_1$, q_2 . . . q_r, where q_1, q_2 . . . q_r are distinct prime numbers, *the sum of the numbers of the series 1, 2 . . . p − 1 which belong to exponent* $p_a^\beta q_1 q_2 \ldots q_r$ *is* $\equiv 0 \pmod{p}$.

We are now in position to prove, by complete induction, that the sum of those numbers of the series 1, 2 . . . p—1 which belongs to an exponent which is divisible by the square of a prime number is always $\equiv 0 \pmod{p}$. In fact we may first prove this for the case when this exponent is of the form $q_1^{\alpha_1} q_2^{\alpha_2}$, q_1 and q_2 being distinct primes, and α_1, $\alpha_2 > 1$. Then we can establish the given result for the case when this exponent is of the form $q_1^{\alpha_1} q_2^{\alpha_2} q_3 q_4 \ldots q_r$ by following the method employed above. After this we establish this result for the exponents which are of the form $q_1^{\alpha_1} q_2^{\alpha_2} q_3^{\alpha_3}$ (α_1, α_2, $\alpha_3 > 1$), and then for the exponents of the form $q_1^{\alpha_1} q_2^{\alpha_2} q_3^{\alpha_3} q_4 \ldots q_r$. As this process can evidently be continued indefinitely, we have established the theorem: *The sum of those numbers of the series 1, 2 . . . p − 1 which belong to any exponent which is divisible by the square of a prime number is always* $\equiv 0 \pmod{p}$, *while the sum of those which belong to an exponent which is not divisible by the square of a prime is* $\equiv 1$ *or* $-1 \pmod{p}$ *as the number of the prime numbers which divide this exponent is even or odd.**

*A little more general theorem is given by Bachmann, *Niedere Zahlentheorie* (1902), p. 402.

§ 4. A Few Deductions.

The given theorems may be used to advantage to find the numbers which belong to certain exponents, especially when the ϕ-function of these exponents is small. Since the reciprocal of any number belongs to the same exponent as the number itself, it results that when the ϕ-function of this exponent is 2 the number and its reciprocal constitute the only numbers which belong to this exponent. In particular, when the number n belongs to exponent 3(mod p) n^2 must belong to the same exponent and $n^2+n\equiv -1 \pmod{p}$. Hence we may say that a necessary and sufficient condition that the number $n>1$ belongs to exponent 3 (mod p) is that $n(n+1)\equiv -1$. Hence n belongs to exponent 3 whenever p is of the form $n(n+1)+1$. The five primes below 100 which are of this form are 7, 13, 31, 43 and 73. Numbers belonging to exponent 3 (mod p) may often be readily obtained by the following method, whose correctness is easily proved: Find the reciprocal r of 4 (mod p) and find by trial the smallest value of k such that $kp+r-1$ is a perfect square. The two numbers $\frac{1}{2}(p-1)\pm\sqrt{(kp+r-1)}$ will then belong to exponent 3. It is clear that p must have the form $6n+1$.

In a similar manner we see that if n belongs to exponent 4, n^3 will belong to this exponent and $n^3+n\equiv 0 \pmod{p}$. Two neccessary and sufficient conditions that the number n belongs to exponent 4 (mod p) are therefore that $n(n^2+1)\equiv 0$, and that n is prime to p. Similarly, we observe that a necessary and sufficient condition that n belongs to exponent 6 (mod p) is that $n+\frac{1}{n}\equiv 1 \pmod{p}$. We may deduce from these results the following useful theorem: *A necessary and sufficient condition that the number n, which is prime to the prime odd number p, belongs to exponents 3, 4, or 6 (mod p) is that the sum of n and its reciprocal is congruent to −1, 0, or 1 respectively.* When this sum is congruent to ± 1, n must be prime to p. Hence we have that a necessary and sufficient condition that n belongs to exponent 3 or 6 (mod p) is that $n+\frac{1}{n}\equiv -1$ or $\equiv 1$, respectively.

ON THE REPRESENTATION OF AN INTEGER AS THE SUM OF CONSECUTIVE INTEGERS.

By THOMAS E. MASON, Indiana University.

Lucas has shown that every number not of the form 2^n can be expressed as the sum of two or more consecutive positive integers. In this paper we shall consider series of consecutive integers and shall not exclude zero and negative terms. It is proposed to find the number of ways in